

Finite-key analysis of the six-state protocol with photon-number-resolution detectors

Silvestre Abruzzo,^{*} Markus Mertz, Hermann Kampermann, and Dagmar Bruß

Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, 40225 Düsseldorf, Germany

(Dated: November 14, 2011)

The six-state protocol is a discrete-variable protocol for quantum key distribution, that permits to tolerate a noisier channel than the BB84 protocol. In this work we provide a lower bound on the maximum achievable key rate of a practical implementation of the entanglement-based version of the six-state protocol. Regarding the experimental set-up we consider that the source is untrusted and the photon-number statistics is measured using photon-number-resolving detectors. We provide the formula for the key rate for a finite initial number of resources. As an illustration of the considered formalism, we calculate the key rate for the setting where the source produces entangled photon pairs via parametric down-conversion and the losses in the channel depend on the distance. As a result we find that the finite-key corrections for the considered scenario are not negligible and they should be considered in any practical analysis.

I. INTRODUCTION

Quantum Key Distribution (QKD) was proposed for the first time in 1984 by Bennett and Brassard[4](BB84 protocol) and it is a method for permitting two parties, usually called Alice and Bob, to share a secret bit-string that might be used as a key for cryptographic applications. The most prominent application is encryption with the one-time pad[25], where Alice sums bitwise the message and the key for obtaining the cypher-text. The cypher-text is then sent to Bob, who recovers the original text by using the knowledge of the key. Note that the encrypted text is sent publicly on the channel and therefore it is readable by any eavesdropper who is tapping the channel. The security of this scheme relies on the fact, that from the eavesdropper's point of view the distribution of all possible cypher-texts is uniform[24]. This last requirement implies that the key is chosen at random using a uniform distribution on the set of all possible keys. This is the point where QKD enters the game. In fact, using the laws of quantum mechanics, it is possible to create a bit-string with the guarantee that it is (almost) random from an eavesdropper's point of view[21]. In this paper we consider the entanglement-based version of the six-state protocol[3, 5, 7, 10]. It has been realized that, due to the use of a tomographic measurement, the six-state protocol is more robust against channel imperfections than the BB84 protocol. The six-state protocol was implemented experimentally, e.g. by Kwiat's group[13]. However, in the meantime the security analysis of this protocol has become more and more complete. In 2001, H.K. Lo[14] proved security of the protocol against the most general type of attacks and some years later R. Renner et al.[9, 12, 19] proved the security of the six-state protocol using information-theoretical arguments. Finite-key effects were considered for the first time by V. Scarani and R. Renner[22, 23] and by T. Meyer et al.[16]. It turns out that there is an initial regime where BB84 is advantageous over the six-state protocol and then there exists a second regime where the six-state protocol leads to higher secret key rates. The reason is the sifting procedure. More precisely, in the standard six-state protocol all measurement bases are chosen with the same probability and as a consequence, $\frac{2}{3}$ of the measurement outcomes are discarded due to this sifting. In the standard BB84 protocol the fraction of discarded outcomes is $\frac{1}{2}$. However, in the year 2005, it was proven by H.K. Lo and M. Ardehali[15] that it is possible to choose one basis with high probability and the other two (one for the BB84) with a negligible probability without jeopardizing the security of the protocol. In the asymptotic case, using this biased scheme, the sifting ratio approaches one and therefore the six-state protocol permits to give a higher secret key rate. However, when finite-key corrections are considered, for small block sizes it is not possible to choose with an arbitrary large bias the measurement basis and therefore the sifting advantage of the BB84 protocol leads to higher key rates. Note that recent papers considering the finite-key analysis studying the six-state protocol[1, 6, 22, 23] do not consider a realistic implementation with imperfections in the source, the channel and the detectors. The security proof becomes more involved due to the fact that a realistic source does have multi-photon pulses, which need special care. A common receipt is given by the squashing model[2], which permits to analyze the security of multi-photon sources using single photons and a special post-processing of the outcomes. However, it was proven that an active measurement set-up for the six-state protocol does not permit to use the squashing model[2]. A squashing model for the passive measurement set-up exists[2], but up to now only in the case of perfect detectors. However, another technique permitting to overcome the need of squashing model has

^{*} abruzzo@thphy.uni-duesseldorf.de

been developed by T. Moroder et al.[17]. The main observation is, that if we had perfect photon-number-resolution detectors (PNRD), then we would be able to avoid the problem of multi-photon pulses by post-selecting only single-photon pulses. In their paper the authors developed an experimentally feasible technique permitting to acquire the statistics of a PNRD. In this paper we want to extend their analysis considering finite-key corrections. In order to state clearly our result, we will consider an ideal set-up, where we perform a Quantum Non-Demolition (QND) measurement permitting to detect error-free the number of photons present in an incoming pulse. We will use a standard measurement set-up, which has detectors with finite efficiency. Note that, although the set-up we consider may be idealized, it permits to provide a lower bound for the performance of the six-state protocol in presence of a realistic scenario. Finally, we will consider a specific example, i.e. we will calculate the secret key rate in the finite case for a spontaneous parametric down-conversion of type-II (SPDC) source.

The paper is organized as follows. In section II we describe the set-up followed by a presentation of the QKD protocol. In section III we present the security analysis and the formula for the secret key rate. In section IV we calculate the optimal secret key rate for a SPDC source. Finally, in section V we conclude this analysis.

II. THE ENTANGLED VERSION OF THE SIX-STATE PROTOCOL

In the first part of this section we present the set-up used by Alice and Bob. The second part considers an outline of the QKD protocol.

A. Set-up (see Fig. 1)

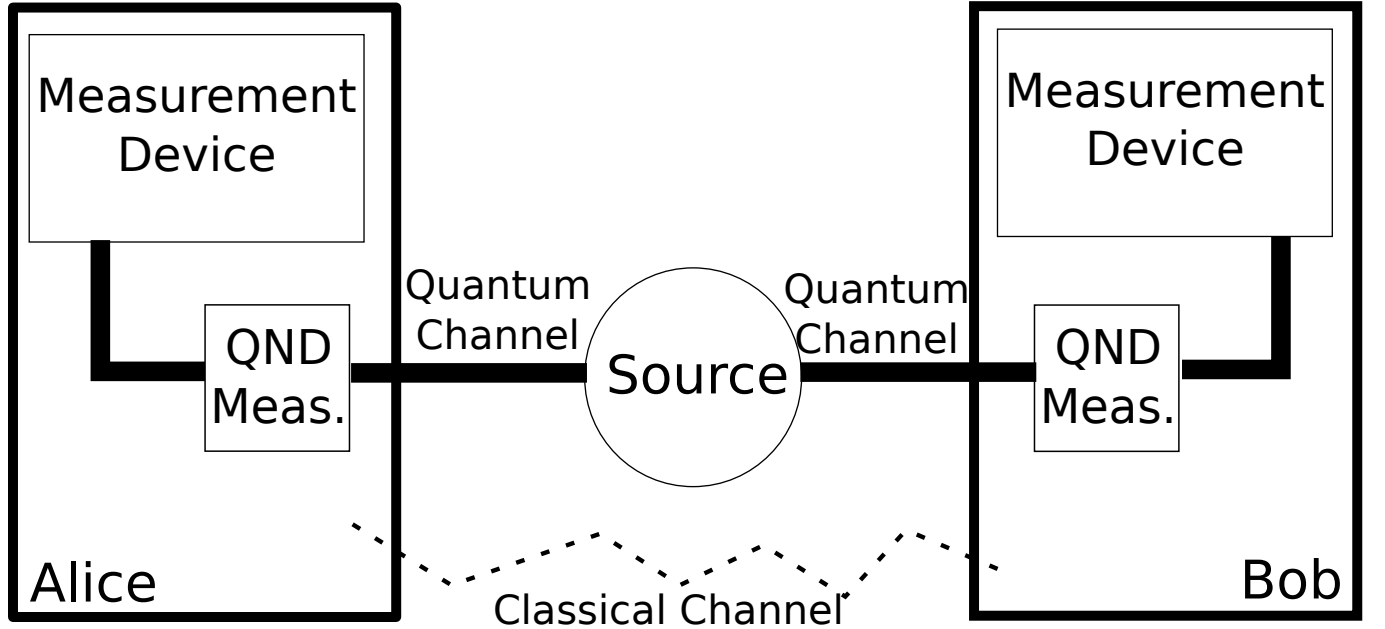


FIG. 1. Set-up for QKD. The quantum channel is completely controlled by the eavesdropper. The classical channel is authenticated but otherwise tapped by the eavesdropper. The laboratories are by definition secure.

- **Source.** An arbitrary source is placed in the middle of Alice and Bob. The source sends an n -photon pulse to Alice and an m -photon pulse to Bob.
- **Quantum Channel.** We consider that the channel is lossy but otherwise error-free. We suppose that the signals are encoded in the source, such that they do not experience any decoherence in the channel.
- **Classical Channel.** The classical channel is authenticated.
- **Alice's (Bob's) laboratory.** We assume that the laboratories are trusted. Alice (Bob) performs a QND measurement for measuring the number of photons contained in the incoming pulse. The POVM of the QND

measurement is composed of two elements $\{|1\rangle\langle 1|, \mathbb{1} - |1\rangle\langle 1|\}$, where $\{|n\rangle\}$ is the Fock-basis. After the QND measurement, the pulse passes a standard QKD-measurement set-up, where one measurement basis is chosen at random out of the X -, Y - and Z -direction. Note that regarding the detectors, we assume that they have finite efficiency η_D and negligible background noise. Moreover, we consider a misalignment[17, 21] in the detectors. Each time that a single photon arrives at the detection device, it is measured correctly with probability $1 - \eta_M$.

B. QKD protocol

1. **Entanglement generation and distribution.** A source generates entangled pairs which are distributed through the quantum channel to Alice and Bob.
2. **Measurement.** Alice and Bob choose at random and independently the measurement basis and to perform the measurement on the incoming pulse. We consider a biased choice of the bases, i.e., the basis Z is chosen with probability $p_Z \geq \frac{1}{3}$ and the other two bases are chosen with the same probability $p_X = p_Y$. The result of the measurements is recorded in a vector of the form $(t^A, b_0^A, b_1^A, p^A, basis^A)$, where $b_i^A = 0$ indicates that the detector for the classical value i on Alice side did not experience a click, otherwise $b_i^A = 1$. The entry p^A contains the result of the QND measurement, in particular $p^A = 1$ when a 1-photon pulse is measured and $p^A = 0$ otherwise. The last entry contains a label for the measurement basis. The first entry t^A is a tag permitting to distinguish the measurements, e.g., the time of occurrence of the measurement.
3. **Vacuum sifting.** During this sifting we remove the non-measurement results. This step is performed locally and without communication between Alice and Bob. Let $i=A,B$. When $p^i = 1$, it is still possible that $b_0^i + b_1^i = 0$, i.e., none of the detectors has clicked. This can happen due to the finite efficiency of the detectors. We can eliminate these events safely, incorporating the efficiency of the detectors in the efficiency of the channel. During this step Alice (Bob) calculate the value of $b_0^i + b_1^i$ and set $p^i = 0$ every time that $b_0^i + b_1^i = 0$.
4. **Pulse sifting.** We use the output of the QND measurement for conditioning the type of bits used for the key. Alice and Bob communicate via the classical channel the value of p^A and p^B for each measurement and discard all measurements with $p^A \times p^B \neq 1$ [17]. Note that this post-processing is possible only due to the fact, that the QND measurement is perfect and that we are considering entanglement-based QKD. If one of the two assumptions above is dropped, then security loopholes will arise[21].
5. **Bases sifting.** Alice and Bob exchange information regarding the measurement bases and discard the outcomes coming from different bases.
6. **Parameter estimation.** Alice and Bob take a random sample from each basis and use this sample for estimating the Quantum Bit Error Rate (QBER) for each basis. We denote with e_{X,m_X} the fraction of erroneous bits in the sample of length m_X . We choose[6] $m_X = m_Y = m_Z := Np_X^2$, where N is the number of bits after the pulse sifting. The QBERs along the Y and Z bases are defined analogously. Note that the worst-case QBER can be estimated with the fluctuations due to the finiteness of the sample.
7. **Error correction.** During this step Alice and Bob apply a one-way error correction protocol and correct their strings. As result they will exchange leak_{EC} bits on the channel.
8. **Error verification.** In realistic implementations it is possible that at the end of the error correction protocol, Alice and Bob do not have perfectly correlated bits. In order to acquire confidence regarding the remaining errors, they apply a two-universal hash function on their strings and they communicate the result of the function on the channel. This step costs $\log_2(\frac{2}{\varepsilon_{EC}})$ bits. If the resulting hash tag is the same, then the two strings are the same with probability $1 - \varepsilon_{EC}$. If the hashing produces a different outcome, Alice and Bob may perform more error correction followed by another error verification.
9. **Privacy amplification.** Alice and Bob apply a two-universal hash function in order to shrink their string. The resulting string is called the key.
In the next section we will discuss a bound on the achievable key length ℓ as a function of a security parameter ε .

III. FINITE SECRET KEY RATE

The secret key rate is the relevant figure of merit for describing the performance of a QKD protocol. First of all, we are going to state the definition of security.

Definition III.1. [18, 20] Let ρ_{KE} be the classical-quantum-state describing the classical key K of length ℓ , distilled at the end of a QKD protocol, correlated with the quantum states of the eavesdropper ρ_E . The state ρ_{KE} is said to be ε -secure if

$$\min_{\rho_{E'}} \frac{1}{2} \|\rho_{KE} - \frac{1}{2^\ell} \mathbb{1} \otimes \rho_{E'}\|_1 \leq \varepsilon, \quad (1)$$

where $\rho_{E'}$ is the quantum state of an eavesdropper not correlated with the key.

The definition states that from the eavesdropper's (Eve) point of view the classical key K is indistinguishable from a random and uniform key with probability $1 - \varepsilon$. Note that the used definition of security is composable, i.e. if we have two protocols characterized by two different probabilities of failure, then, after a concatenation of these protocols, the probability of failure of the global protocol will be bounded by the sum of the single probabilities of failure.

In the following we derive a formula for the ε -secure key length ℓ . We consider that Eve has complete control over the quantum channel and the source. Moreover, we consider the *uncalibrated scenario* [21], where the finite efficiency of the detectors are also attributed to Eve. Let p_{11} be the probability that Alice and Bob receive a single photon. Then, starting with N_{source} initial pulses, the steps 1 – 4 of the QKD protocol (see Fig. 1) decrease the number of signals to $N_{\text{source}} p_{11}$. Afterwards, the bases-sifting and the PE lead to $N_{\text{source}} p_{11} (p_Z^2 - p_X^2)$ resulting bits. For PE $3p_X^2$ signals are used to estimate the QBER. The fluctuations due to finite statistics have been analyzed in [6, 8, 22, 23]. Note that differently to [6] we do not consider one symmetrized QBER. Instead we treat the QBER for each direction separately.

Let e_{i,m_i} be the measured QBER in direction $i = X, Y, Z$, then with probability $1 - \varepsilon_{PE}$ the real QBER e_i is such that [6, 8, 22, 23]

$$e_i \leq e_{i,m_i} + 2\zeta(\varepsilon_{PE}, m_i) \quad (2)$$

with

$$\zeta(\varepsilon_{PE}, m) := \sqrt{\frac{\ln\left(\frac{1}{\varepsilon_{PE}}\right) + 2 \ln(m+1)}{8m}}. \quad (3)$$

For the error correction protocol the total number of bits exchanged during the procedure is an upper bound on the information leaked to the eavesdropper about the final key. For the simulations, we will use [8, 23]

$$\text{leak}_{\text{EC}} := f_{\text{EC}} n h(e), \quad (4)$$

where $f_{\text{EC}} \geq 1$ depends on the used EC protocol, $h(e)$ is the binary Shannon entropy, i.e., $h(e) = -e \log e - (1 - e) \log(1 - e)$ and e is the QBER. This definition comes from the fact that $nh(e)$ represents the asymptotic number of bits used by a perfect error correction protocol. The coefficient f_{EC} represents a deviation of the real protocol from the asymptotic one.

Regarding privacy amplification many bounds on the achievable secret key length are placed at the disposal in the literature [1, 6, 22, 23]. Note that the bounds given in [1, 6] are tighter than the bound given in [22, 23]. However, they require that the channel is symmetric. Although it is possible to transform any channel in a symmetric one, we consider the bound provided in [22, 23] to take the analysis simple and more general.

The following result summarizes the preceding considerations and provides a formula for the achievable secret key length. It is important to emphasize, that the following theorem holds only due to our special set-up with the QND measurement and the particular post-processing, which selects only the pulses containing one photon.

Theorem III.2 ([22, 23]). *Let N_{source} being the number of measurements performed by Alice and Bob. Let p_{11} be the fraction of attempts resulting in a single-photon pulse entering Alice's and Bob's laboratories. The number of bits allocated for extracting a key is $n := N_{\text{source}} p_{11} (p_Z^2 - p_X^2)$. If Alice and Bob distill a key of length*

$$\ell \leq \max_{\varepsilon, \varepsilon_{PE}, \varepsilon_{PA}, p_X, p_{11}} \left[n(S_\zeta(X|E) - f_{\text{EC}} h(e_Z)) - 2 \log_2 \frac{1}{\varepsilon_{PA}} - \log_2 \frac{2}{\varepsilon_{\text{EC}}} \right], \quad (5)$$

then it is ε -secure, with $0 \leq \bar{\varepsilon} + \varepsilon_{EC} + \varepsilon_{PA} + \varepsilon_{PE} \leq \varepsilon$. The quantity $S_\zeta(X|E)$ is given by [21–23]

$$S_\zeta(X|E) := 1 - e_Z h\left(\frac{1 + (e_X - e_Y)/e_Z}{2}\right) - (1 - e_Z) h\left(\frac{1 - (e_X + e_Y + e_Z)/2}{1 - e_Z}\right) - 5\sqrt{\log_2\left(\frac{2}{\bar{\varepsilon}}\right)\frac{1}{n}}. \quad (6)$$

The entropy $S_\zeta(X|E)$ is calculated with the QBER inferred during the parameter estimation protocol (see Eq. (2)). We would like to point out that the theorem above is a standard theorem, the unique difference is that we are not using all signals for extracting the key but only the signals coming as single-photon pulse.

The asymptotic formula for the secret key rate can be recovered as a special case of the theorem above for $n \rightarrow \infty$ and $\varepsilon \rightarrow 0$.

IV. CASE STUDY: SPDC SOURCE

In this section we will calculate the achievable secret key length for a pumped type-II down-conversion source[11]. The produced state by this source can be written as

$$|\phi\rangle_{AB} := \sum_{n=0}^{\infty} \sqrt{p_n} |\phi_n\rangle_{AB}, \quad (7)$$

where

$$p_n := \frac{(n+1)\lambda^n}{(1+\lambda)^{n+2}}, \quad (8)$$

and

$$|\phi_n\rangle_{AB} := \sum_{m=0}^n \frac{(-1)^m}{\sqrt{n+1}} |n-m, m\rangle_A |m, n-m\rangle_B. \quad (9)$$

The state above is written along one fixed direction, e.g. the Z -direction. The meaning of the notation $|l_H, l_V\rangle_A$ is that on Alice side, a pulse with $l_H + l_V$ photons is coming and $l_H(l_V)$ have horizontal (vertical) polarization.

The quantity 2λ represents the mean photon pair number per pulse.

In the following we calculate the quantities that enter the formula of the secret key rate (Eq. (5)). First of all, we express the probability that Alice and Bob receive only one photon. Then we calculate the QBER produced by the incoming pulse and finally, we find the optimal mean photon pair number per pulse, i.e. the one which maximize the secret key rate.

A. Calculation of p_{11}

We denote with η_A the total transmittivity of Alice's set-up. It is given by $\eta_A := \eta_D \eta_C(L/2)$, where η_D is the efficiency of Alice's detectors and L is the distance between Alice and Bob. We consider a lossy, but otherwise perfect channel with attenuation coefficient $\alpha = 0.17$ dB/km, such that the transmission probability of a photon is given by $\eta_C(L) := 10^{-\frac{\alpha L}{10}}$.

Analogously we define the total efficiency on Bob's set-up, denoted by η_B . When an n -photon pulse is produced, during its travel on the channel and during the detection, some photons could be absorbed. The following formula gives the probability that an n -photon pulse becomes a 1-photon pulse,

$$W_n := p_n n^2 (1 - \eta_A)^{n-1} (1 - \eta_B)^{n-1} \eta_A \eta_B. \quad (10)$$

The factor n^2 is a combinatorial factor coming from our ignorance which photon was absorbed. The total probability that both, Alice and Bob, receive one photon is given by

$$p_{11} := \sum_{n=1}^{\infty} W_n. \quad (11)$$

B. Calculation of the QBER

In the six-state protocol measurements are performed along three orthogonal directions in the Bloch sphere, and, as explained above, three QBERs are involved. The Hamiltonian of the parametric down-conversion process is invariant under rotations from the X- to Y-, Y- to Z- and Z- to X-basis. Therefore, the state in Eq. (7) remains invariant in form under these transformations and hence the QBER is the same in all directions, i.e., there is only one QBER to consider, e.g., for the Z-direction. There are two contributions to the QBER. The first one comes from the misalignment and the second one is due to the fact, that the entering state is not maximally entangled. Let e_n be the QBER generated by $|\phi_n\rangle$ when misalignment is not considered. Then the total QBER is given by

$$e_{PDC} := \frac{\sum_{n=1}^{\infty} (e_M(1 - e_n) + (1 - e_M)e_n)W_n}{p_{11}}, \quad (12)$$

where $e_M := 2\eta_M(1 - \eta_M)$ and η_M is the misalignment-error probability. The first term of e_{PDC} accounts for the fact, that even if the incoming state did not produce a QBER, due to the misalignment there would be an error. The second contribution comes from the error generated by the incoming photons. Note that terms of the form $e_M e_n$ are not considered, because the simultaneous appearance of these two errors will produce correlated outcomes. The quantity e_n can be calculated with the help of Eq. (9). This state is the superposition of $n + 1$ states. The first and the last term in the summation, with $m = 0$ or $m = n$ will produce a correlated outcome. On the contrary the remaining $n - 1$ elements in the summation will produce an error with probability $\frac{1}{2}$. Therefore we get

$$e_n = \frac{(n + 1) - 2}{2(n + 1)} = \frac{1}{2} \left(1 - \frac{2}{n + 1} \right). \quad (13)$$

From the formula above it is possible to verify that $e_1 = 0$, which is consistent with the fact that $|\phi_1\rangle$ is a maximally entangled state.

The common free parameter in the QBER e_{PDC} and in p_{11} is the mean number of photons per pulse 2λ .

Therefore, in the following we will calculate the optimal λ permitting to maximize the secret key rate.

As shown in Fig. 2, in order to have a low QBER e_{PDC} it is necessary to have λ small. For short distances, e.g. $L = 20\text{km}$ it is possible to choose $\lambda < 20$ and at the same time be able to extract a key. The reason is that the multi-photon pulses arrives to Alice and Bob without an appreciable degradation and therefore, we are able to filter those contribution to the QBER during the pulse sifting. However, the situation changes when the distance between Alice and Bob increases. We see that the mean number of photons per pulse has to be much smaller than 1 in order to decrease the multi-photon contribution to the QBER. From Fig. 2 we see that for $L \geq 100\text{km}$ we have to choose $\lambda < 1$ in order to have a QBER smaller than the maximal QBER tolerated by the six-state protocol.

C. Asymptotic secret key rate

The secret key rate in the asymptotic case characterizes the maximal achievable secret key rate in case of perfect error correction, no uncertainty in the estimation of the QBER and perfect security ($\epsilon = 0$). The formula is given by

$$r_{\infty} := \lim_{\substack{n \rightarrow \infty \\ \epsilon \rightarrow 0}} \frac{l}{N_{\text{source}}} = \max_{\lambda} \left[p_{11} \left((1 - e_{PDC}) \left(1 - h \left(\frac{1 - 3e_{PDC}/2}{1 - e_{PDC}} \right) \right) - h(e_{PDC}) \right) \right]. \quad (14)$$

In Fig. 3 the secret key rate is shown as a function of the distance for two different experimental set-ups. A comparison between an idealized scenario ($\eta_D = 1, \eta_M = 0$) and a more realistic one ($\eta_D = 0.1, \eta_M = 0.03$) shows that the secret key rate decreases of at least 2 orders of magnitude. Regarding the optimal mean of photon-number per pulse, as shown in Fig. 4, the difference is of the order of 1. The optimized function is non-linear and the used optimization algorithm may only permit to find a local optimum.

Finally, we would like to point out, that a similar analysis of the asymptotic case was performed by Moroder et al.[17] with a source placed in an asymmetric position, i.e., closer to Bob than to Alice.

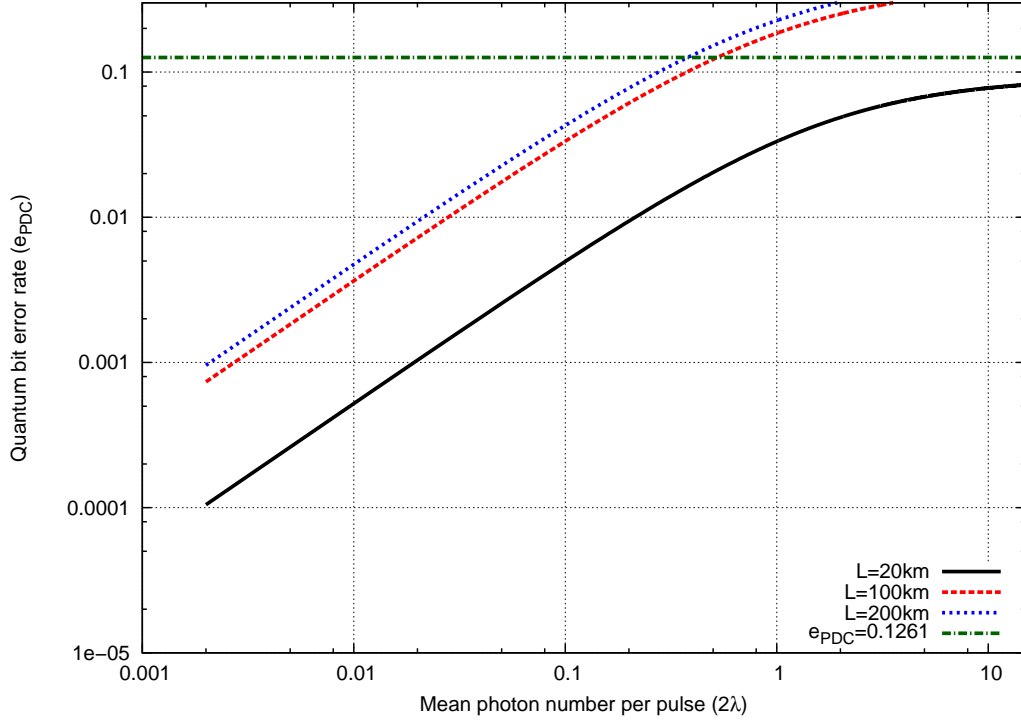


FIG. 2. (Color online) Value of e_{PDC} (Eq. (12)) as a function of the probability that both, Alice and Bob, receive one photon as a function of the mean number of photons produced by the source for various distances. The horizontal line represents the maximal QBER tolerated by the six-state protocol. The absorption of the channel is $\alpha = 0.17$ dB/km and Alice and Bob use perfect detectors $\eta_D = 1, \eta_M = 0$.

D. Finite-key analysis

In a practical execution of a QKD protocol, the initial number of resources is always finite, therefore we need to take into account corrections to the asymptotic secret key rate. The formula for the secret key rate is

$$r := \frac{\ell}{N_{\text{source}}} = \max_{\bar{\varepsilon}, \varepsilon_{PE}, \varepsilon_{PA}, p_X, \lambda} \left[p_{11}(p_Z^2 - p_X^2) \left((1 - e_{PDC}) \left(1 - h \left(\frac{1 - 3e_{PDC}/2}{1 - e_{PDC}} \right) \right) - f_{ECh}(e_Z) \right) \right] \quad (15)$$

$$- 2 \log_2 \frac{1}{\varepsilon_{PA}} - \log_2 \frac{2}{\varepsilon_{EC}} - 5 \sqrt{\log_2 \left(\frac{2}{\bar{\varepsilon}} \right)}. \quad (16)$$

The calculations are done in such a way, that we optimize over all free parameters: the mean number of photons per pulse (λ), the probability to measure along the Z basis (p_Z), the failure probability for the parameter estimation (ε_{PE}), for privacy amplification (ε_{PA}) and the smoothing parameter ($\bar{\varepsilon}$).

For extracting a key it is necessary to have a block bigger than a specific length. As shown in Fig. 5, even for short distances the source has to emit at least 10^5 pulses with in mean $\lambda \approx 0.1$ photons per pulse for extracting a key of 1 bit. However, if we consider detector inefficiencies and misalignment errors, the requirements will become much more stringent. In particular, we need at least 10^9 pulses for extracting a key.

The second quantity we want to analyze is the secret key rate (Eq. (5)). As shown in Fig. 6, for a perfect set-up ($\eta_D = 1, \eta_M = 0$) the finite secret key rate differs significantly from the asymptotic secret key rate. In particular, for all distances considered in Fig. 6, the secret key rate differs of at least 10% ($N_{\text{source}} = 10^{10}$, $L = 20$ km) from the asymptotic key rate. However, for more realistic initial number of pulses, the difference is bigger, e.g for $L = 100$ km and $N_{\text{source}} = 10^8$, the difference between the asymptotic secret key rate and the one with finite-key corrections is of one order of magnitude. In case of imperfections we will have similar plots but with a worse secret key rate. However, the qualitative behavior of the plot remains similar to Fig. 6.

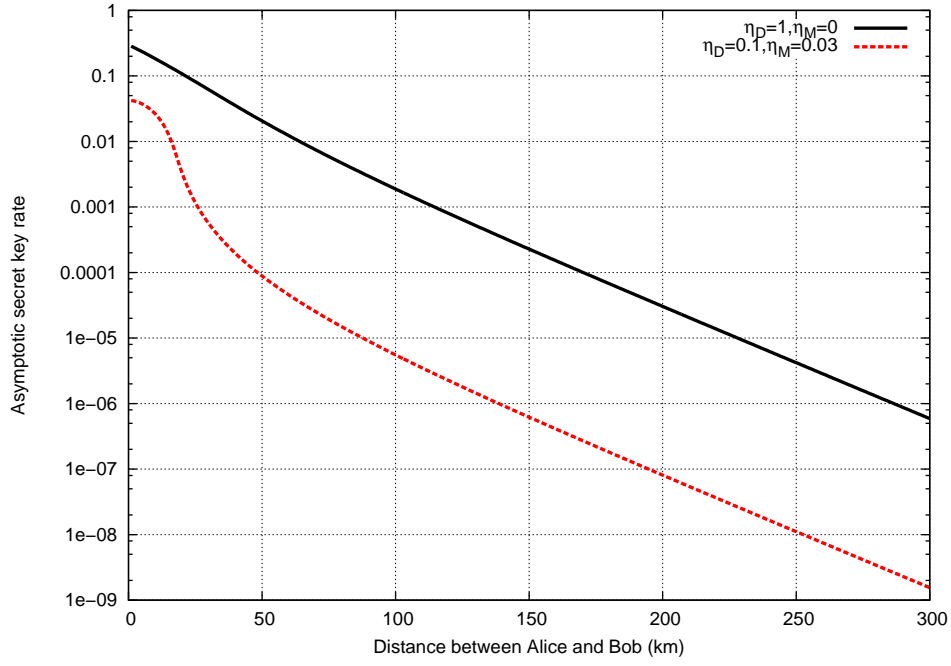


FIG. 3. (Color online) Asymptotic secret key rate (Eq. (14)). The absorption of the channel is $\alpha = 0.17$ dB/km.

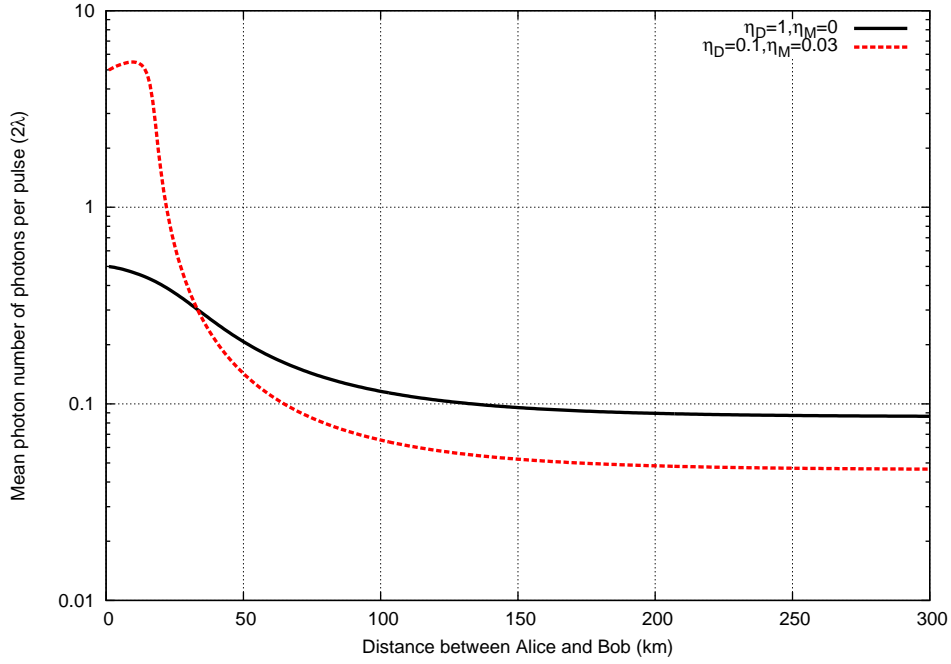


FIG. 4. (Color online) Optimal mean of photon-number per pulse. The absorption of the channel is $\alpha = 0.17$ dB/km.

V. CONCLUSION

In this paper we did a step towards the analysis of a realistic implementation of the entanglement-based version of the six-state protocol. We considered that the standard QKD measurement is preceded by a QND measurement permitting to know the number of photons entering in the source. This special set-up with a post-processing which

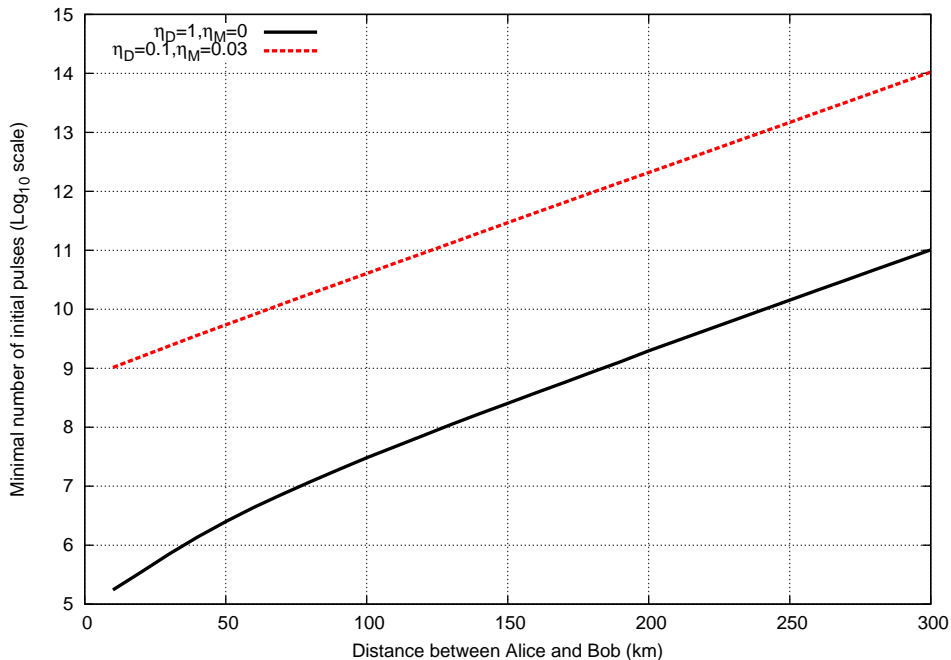


FIG. 5. (Color online) Minimal number of initial pulses permitting to extract a key of 1 bit as a function of the length L for a perfect set-up ($\eta_D = 1$, $\eta_M = 0$). The absorption of the channel is $\alpha = 0.17$ dB/km. Security parameter $\varepsilon = 10^{-9}$, $\varepsilon_{EC} = 10^{-10}$, $f_{EC} = 1.2$.

considers only signals coming from a single-photon source permits to evaluate secret key rates for the six-state protocol. We studied the case of an arbitrary large number of initial pulses as well as of a finite key. As result we found that in realistic implementations with finite-efficiency detectors and misalignment, the minimal number of pulses for being able to extract a key is around 10^9 pulses at the distance of a few kilometers. Note that this is a very stringent requirement. In fact, considering an ordinary source, which emits pulses at the rate of 10 MHz, at the distance of 20 km between Alice and Bob, the time needed for extracting a key of 1 bit will be of the order of 100 seconds. Using the asymptotic key formula, in the same time, it could be possible to obtain a key of length 10^6 bits, which would be unfortunately completely insecure. Therefore, we emphasize once again that finite-key corrections are necessary for a realistic and correct security analysis.

Regarding future work, we underline that more realistic experimental imperfections should be taken into account in order to characterize the performance of the six-state protocol. In a future work, we want to consider the encoding of the quantum bits on the quantum channel and to study the effects of decoherence. This is a problematic issue which limits practical implementations of the six-state protocol and needs a careful analysis.

ACKNOWLEDGMENTS

We would like to thank Sylvia Bratzik and Tobias Moroder for valuable and enlightening discussions. We acknowledge partial financial support by Deutsche Forschungsgemeinschaft (DFG) and by BMBF (project QuOREP).

-
- [1] Abruzzo, S., Kampermann, H., Mertz, M., and Bruß, D. (2011). Quantum key distribution with finite resources: Secret key rates via rényi entropies. *Physical Review A*, 84(3):032321.
 - [2] Beaudry, N. J., Moroder, T., and Lütkenhaus, N. (2008). Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.*, 101(9):093601.
 - [3] Bechmann-Pasquinucci, H. and Gisin, N. (1999). Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Phys. Rev. A*, 59(6):4238–4248.

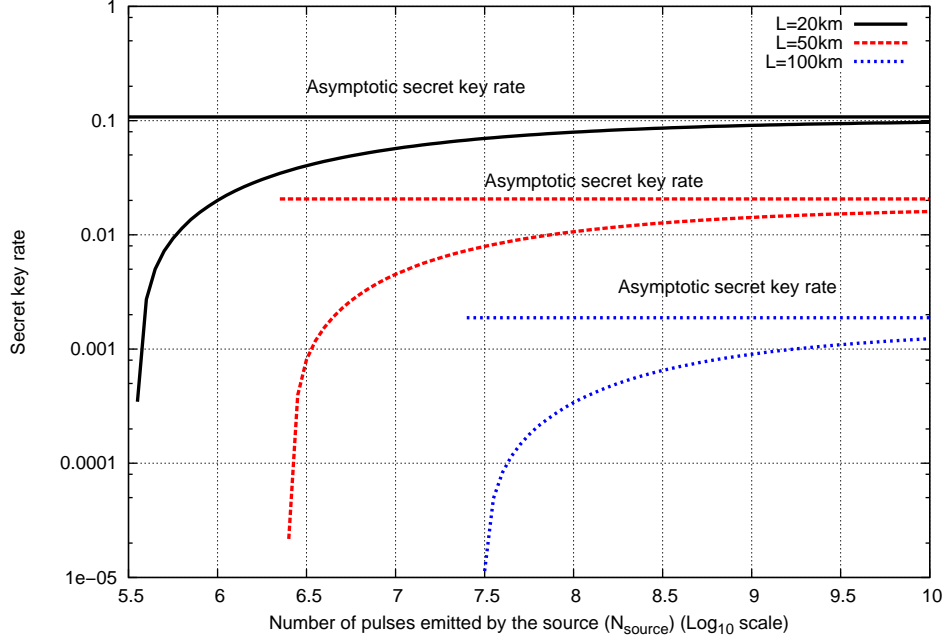


FIG. 6. (Color online) Secret key rate as a function of the number of pulses emitted by the source (N_{source}) for a perfect set-up ($\eta_D = 1$, $\eta_M = 0$). The absorption of the channel is $\alpha = 0.17$ dB/km. Security parameter $\varepsilon = 10^{-9}$, $\varepsilon_{\text{EC}} = 10^{-10}$, $f_{\text{EC}} = 1.2$.

- [4] Bennett, C. and Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175. Bangalore, India.
- [5] Bennett, C., Brassard, G., and Mermin, N. (1992). Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68(5):557–559.
- [6] Bratzik, S., Mertz, M., Kampermann, H., and Bruß, D. (2011). Min-entropy and quantum key distribution: Nonzero key rates for “small” numbers of signals. *Phys. Rev. A*, 83(2):022330.
- [7] Bruß, D. (1998). Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81(14):3018–3021.
- [8] Cai, R. Y. Q. and Scarani, V. (2009). Finite-key analysis for practical implementations of quantum key distribution. *New Journal of Physics*, 11(4):045024.
- [9] Christandl, M., Renner, R., and Ekert, A. (2004). A generic security proof for quantum key distribution. *Arxiv preprint quant-ph/0402131*.
- [10] Ekert, A. (1991). Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663.
- [11] Kok, P. and Braunstein, S. L. (2000). Postselected versus nonpostselected quantum teleportation using parametric down-conversion. *Phys. Rev. A*, 61(4):042304.
- [12] Kraus, B., Gisin, N., and Renner, R. (2005). Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.*, 95(8):080501.
- [13] Kwiat, P., Enzer, D. G., Hadley, P. G., and Peterson, C. G. (2001). Experimental six-state quantum cryptography. In *International Conference on Quantum Information*, page FQIPB4. Optical Society of America.
- [14] Lo, H. (2001). Proof of unconditional security of six-state quantum key distribution scheme. *Quantum Information and Computation*, 1(2):81–94.
- [15] Lo, H.-K., Chau, H., and Ardehali, M. (2005). Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology*, 18:133–165.
- [16] Meyer, T., Kampermann, H., Kleinmann, M., and Bruß, D. (2006). Finite key analysis for symmetric attacks in quantum key distribution. *Phys. Rev. A*, 74(4):042340.
- [17] Moroder, T., Curty, M., and Lütkenhaus, N. (2009). Detector decoy quantum key distribution. *New Journal of Physics*, 11(4):045008.
- [18] Müller-Quade, J. and Renner, R. (2009). Composability in quantum cryptography. *New Journal of Physics*, 11(8):085006.
- [19] Renner, R., Gisin, N., and Kraus, B. (2005). Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72(1):012332.
- [20] Renner, R. and König, R. (2005). Universally composable privacy amplification against quantum adversaries. In Kilian, J., editor, *Theory of Cryptography*, volume 3378 of *Lecture Notes in Computer Science*, pages 407–425. Springer Berlin / Heidelberg.

- [21] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M. (2009). The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81(3):1301–1350.
- [22] Scarani, V. and Renner, R. (2008a). Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100(20):200501.
- [23] Scarani, V. and Renner, R. (2008b). Security bounds for quantum cryptography with finite resources. In Kawano, Y. and Mosca, M., editors, *Theory of Quantum Computation, Communication, and Cryptography*, volume 5106 of *Lecture Notes in Computer Science*, pages 83–95. Springer Berlin / Heidelberg.
- [24] Shannon, C. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715.
- [25] Vernam, G. (1926). Cipher printing telegraph systems for secret wire and radio telegraphic communications. *American Institute of Electrical Engineers, Transactions of the*, 45:295–301.